## AMENDMENTS TO THE CLAIMS

**Listing of the Claims:**

Claim 1 (Currently Amended): A method for providing a time stamp by using a tamper-proof time signal via a telecommunications network comprising the steps of:

receiving, at a central system, a request from one of a plurality of network users for a time signal, the central system comprising a plurality of clock systems, wherein each of the plurality of clock systems of the central system is uniquely assigned to one of the plurality of network users, the request including an identifier uniquely assigned to the network user;

identifying, by the central system based on the received identifier uniquely assigned to the network user, one of the plurality of clock systems thereof uniquely assigned to the network user;

encrypting said time signal by the central system with at least one key obtained from the clock system uniquely assigned to the network user;

transmitting the encrypted time signal to the one of the plurality of network user assigned to the identified clock system via the telecommunications network; and

synchronously creating the at least one key by the clock system of the central system uniquely assigned to the network user and a clock system of the network user corresponding to the uniquely assigned clock system of the central system.

Claim 2 (Previously Presented): The method as recited in claim 1, wherein the synchronously creating is performed so as to change the at least one key synchronously after predetermined time intervals.

Claim 3 (Canceled).

Claim 4 (Previously Presented): The method as recited in claim 1, further comprising the steps of:

determining, by the central system, the clock system uniquely assigned to the network user using a transmitted identifier, wherein the transmitted identifier is the network address of the network user.

Claim 5 (Previously Presented): A method for transmitting data with a tamper-proof time stamp over a telecommunications network from a first network user to a second network user, comprising the steps of:

obtaining a time signal in accordance with a method as recited in claim 1;

transmitting the time signal and the data from the first network user to the second network user one of directly and indirectly via the central system.

Claim 6 (Previously Presented): The method as recited in claim 5, further comprising the steps of:

encrypting, by the first network user, at least one of the data and the time signal during transmission.

Claim 7 (Previously Presented): The method as recited in claim 5, wherein the central system is provided at the second network user.

Claim 8 (Previously Presented): The method as recited in claim 5, further comprising the step of returning, by the central system, an acknowledgement of receipt to the first network user.

Claim 9 (Currently Amended): A system for generating a tamper-proof time stamp in network-based communication systems, the system comprising:

a central system connected to the network-based communication system, the central system comprising a plurality of clock systems; and

a plurality of network users connected to the network-based communication system, each of the plurality of network users comprises a clock system, wherein each of the clock systems at the central system is uniquely assigned to one of the plurality of network users,

wherein the clock system of each network user and the respective clock system of the central system are configured to operate synchronously so as to create at least one changeable key,

wherein the central system is configured to receive a request from one of the plurality of network users and encrypt a time signal using the at least one changeable key obtained from one of the plurality of clock systems uniquely assigned to the network user, the request

including an identifier uniquely assigned to the network user, ~~and~~ the central system further configured to send the encrypted time signal to the network user, and further configured to identify, based on the received identifier uniquely assigned to the network user, one of the plurality of clock systems thereof uniquely assigned to the network user; and

wherein the network user is configured to decrypt the encrypted time signal.

Claim 10 (Previously Presented): The system as recited in claim 9, wherein the central system includes a time signal transmitter.

Claim 11 (Canceled).

Claim 12 (Previously Presented): The method as recited in claim 6, wherein a central system is provided at the second network user.

Claim 13 (Previously Presented): The method as recited in claim 6, wherein the central system is configured to return an acknowledgement of receipt to the first network user.

Claim 14 (Previously Presented): The method as recited in claim 7, wherein the central system is configured to return an acknowledgement of receipt to the first network user.

Claim 15 (Previously Presented): The method as recited in claim 1, further comprising the step of decrypting, by the network user using the at least one key, the transmitted encrypted time signal.

Claim 16 (Previously Presented): The method as recited in claim 1, wherein the central system is a certified central system.

Claim 17 (Previously Presented): The method as recited in claim 1, wherein the time signal is an officially recognized time signal.

Claim 18 (Previously Presented): The method as recited in claim 4, wherein the at least one key is created by the uniquely assigned clock system based on the transmitted identifier.

Claim 19 (Previously Presented): The system as recited in claim 9, wherein the at least one-changed key is synchronously created at intervals of time.

Claim 20 (Previously Presented): The system as recited in claim 9, wherein the time signal is an officially recognized time signal.

Claim 21 (New): The method as recited in claim 1, further comprising determining, by the central system, the location of the network user based on an identifier uniquely assigned to the network user.

Claim 22 (New): The system as recited in claim 9, wherein the central system is further configured to determine the location of the network user based on an identifier uniquely assigned to the network user.